HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

10017334-1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Richard P. Tarquini et al.

Application No.: 10/003,820

Confirmation No.: 4709

Filed: October 31, 2001

Art Unit: 2136

For: NODE, METHOD AND COMPUTER READABLE MEDIUM FOR OPTIMIZING PERFORMANCE OF SIGNATURE RULE MATCHING IN A NETWORK

Examiner: C. G. Colin

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

As required under 37 CFR §41.37(a), this brief is filed within two months of the Notice of Appeal filed in this case on November 14, 2006, and is in furtherance of said Notice of Appeal.

The fees required under 37 C.F.R. §41.20(b)(2) were submitted in the original Transmittal of Appeal Brief filed January 2, 2006. However, if a fee is due, please charge our Deposit Account No. 08-2025, under Order No. 10017334-1, from which the undersigned is authorized to draw.

This brief contains items under the following headings as required by 37 C.F.R. §41.37 and M.P.E.P. §1206:

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

Hewlett-Packard Development Company, L.P., a Limited Partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249, Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 20 claims pending in application.

B. Current Status of Claims

1. Claims canceled: none
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 1-20
4. Claims allowed: none
5. Claims rejected: 1-20

C. Claims On Appeal

The claims on appeal are claims 1-20

IV. STATUS OF AMENDMENTS

A Final Office Action rejecting the claims of the present application was mailed October 24, 2006. In response, Applicant did not file an Amendment After Final Rejection, but instead filed a Notice of Appeal, which this brief supports. Accordingly, the claims on appeal are those as rejected in the Final Office Action of October 24, 2006. A complete listing of the claims is provided in the Claims Appendix hereto.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the separately argued claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. §41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. It should be noted that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

According to one claimed embodiment, such as that of independent claim 1, a node (85) of a network (100) for managing an intrusion protection system, the node (85) comprising: a memory module (274) for storing data in machine-readable format for retrieval and execution by a central processing unit (272); and an operating system (275) comprising a network stack (90) comprising a protocol driver (135) and a media access control driver (145) and operable to execute an intrusion protection system management application (279), the management application operable to receive text-file (277A-277N) input from an input device (281), the text-file (277A-277N) defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule (at least page 17, line 8 – page 21, line 2).

In certain embodiments, such as that of dependent claim 2, the at least one field comprises a field selected from the group consisting of an ENABLED field and a SEVERITY field (at least page 17, line 8 – page 21, line 2).

In certain embodiments, such as that of dependent claim 3, the node (85) is operable to compile the text-file (277A-277N) into a machine-readable signature-file (281A-281N) and transmit the machine-readable signature-file to at least one other node (270) of the network (at least page 17, line 8 – page 21, line 2).

In certain embodiments, such as that of dependent claim 5, the node (85) further comprises a machine-readable signature-file database (278B) operable to store a plurality of machine-readable signature-files (281A-281N) each generated from one of a respective plurality of text-files (277A-277N), the management application (279) operable to transmit a subset of the plurality of machine-readable signature-files (281A-281N) to another node (270) connected to the network (100). In certain embodiments, such as that of dependent claim 6, the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files (281A-281N) each generated from a respective text-file (277A-277N) having an asserted ENABLED field value (at least page 17, line 8 – page 21, line 2).

In certain embodiments, such as that of dependent claim 7, the management application (279) is operable to accept a SEVERITY threshold from the input device (281) and the subset comprises all machine-readable signature-files (281A-281N) respectively generated from a text-file (277A-277N) having a SEVERITY field value equal to or greater than the threshold (at least page 17, line 8 – page 21, line 2).

According to one claimed embodiment, such as that of independent claim 8, a method of distributing command and security updates in a network (100) having an intrusion protection system (91) comprising generating a text-file (277A-277N) defining a network-exploit rule, and specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file (277A-277N), *see* at least page 17, line 8 – page 21, line 2.

In certain embodiments, such as that of dependent claim 11, the subset of machine-readable signature-files (281A-281N) comprises all of the plurality of machine-readable signature-files each generated from a respective one of the plurality of text-files (277A-277N) that has the respective ENABLED field asserted (at least page 17, line 8 – page 21, line 2).

In certain embodiments, such as that of dependent claim 12, the method further comprises specifying a priority level threshold, the subset of the plurality of machine-readable signature-files (281A-281N) comprised of all machine-readable signature-files generated from a

respective one of the plurality of text-files (277A-277N) having a SEVERITY level field value equal to or greater than the threshold (at least page 17, line 8 – page 21, line 2).

According to one claimed embodiment, such as that of independent claim 13, a computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor (272), cause the processor (272) to perform a computer method of reading input from an input device (281) of the computer; compiling the input into a machine-readable signature file (281A-281N) comprising machine-readable logic representative of a network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field, evaluating the machine-readable signature file (281A-281N), and determining the value of the at least one field of the machine-readable signature file (281A-281N), *see* at least page 17, line 8 – page 21, line 2.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claim 1 and the intervening claims are rejected under 35 USC §112, second paragraph, as failing to set forth the subject matter which applicant regards as his invention.

Claims 8, 13-14, and 16 are rejected under 35 USC §102(e) as being anticipated by U.S. Patent 6,728,885 to Taylor et al. (hereinafter "*Taylor*").

Claims 1-7, 9-12, 15, and 17-20 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Taylor* in view of U.S. Patent 5,987,611 to Freund (hereinafter "*Freund*").

VII. ARGUMENT

Appellant respectfully traverses the outstanding rejections of the pending claims, and requests that the Board reverse the outstanding rejections in light of the remarks contained herein. The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-heading as required by 37 C.F.R. § 41.37(c)(1)(vii).

A. Rejections under 35 U.S.C. §112, Second Paragraph

Independent claim 1 recites:

> A node of a network for managing an intrusion protection system, the node comprising:
> a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit; and
> an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application, the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule.

The Final Office Action asserts that this claim fails to set forth the subject matter which applicant regards as the invention. In support of this assertion, the Final Office Action explains:

> Evidence that claim 1 fail(s) to correspond in scope with that which applicant(s) regard as the invention can be found in the reply filed on 8/7/2006. In that paper, applicant has stated determination is made as to whether a network exploit rule in the configuration file is to be evaluated, which can lead to inefficient processing if rules are defined that are not desired to be evaluated, and this statement indicates that the invention is different from what is defined in the claim(s) because the claimed invention recites "a determination is made as to whether an intrusion protection evaluates the network exploit rule". (Emphasis original).

Appellant is unclear as to what the Examiner is contending in this rejection. Claim 1 recites in part "the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule." The response of 8/7/2006 argues (on page 8 thereof) that *Taylor* fails to teach at least this element of claim 1 as follows:

> *Taylor* does not teach that the configuration file comprises at least one field that includes information from which a determination is made as to whether an IPS evaluates the network-exploit rule. No determination of whether an intrusion protection system is to evaluate a rule is made in *Taylor*, but instead *Taylor* appears to teach that all rules defined in its configuration file are all evaluated irrespective of any information contained in the configuration file. Again, when evaluated, a determination may be made that a rule is not satisfied under certain circumstances, and thus the corresponding actions (e.g., filtering packets) may not be applied; but in all cases of *Taylor* all rules defined in the configuration file appear to be evaluated.
>
> Thus, *Taylor* does not provide any teaching whatsoever of including at least one field in its configuration file from which a determination is made as to whether a network-exploit rule in the configuration file is to be evaluated by an IPS, which potentially leads to inefficient processing if rules are defined in the configuration file that are not desired to be evaluated, *see e.g.,* page 17, line 8 – page 21, line 2 of the specification of the present application.

Nothing argued by Appellant in the 8/7/2006 is inconsistent with the scope of claim 1, but instead the arguments are fully consistent with the express language provided in claim 1. That is, claim 1 expressly recites that the text-file defines a network-exploit rule and comprises at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule. Appellant argued in the 8/7/2006 response that *Taylor* fails to teach such a field in a text-file, and argued that as explained in the present application that a failure to determine whether an IPS is to evaluate the network-exploit rule from such a field in the text-file leads to inefficient processing because there may be rules defined in the configuration file that are not desired to be evaluated by the IPS but which the IPS nevertheless evaluates.

Accordingly, Appellant respectfully submits that the language of claim 1 is sufficiently definite under 35 U.S.C. §112, second paragraph, and is not inconsistent with the description in the specification or the arguments raised by the 8/7/2006 response. Therefore, Appellant respectfully requests that this rejection be overturned.

B. Rejections under 35 U.S.C. §102 over *Taylor*

As an initial matter, it is unclear exactly which claims stand rejected under 35 U.S.C. §102(e) as being anticipated by *Taylor*. In the non-final Office Action mailed April 7, 2006, claims 1-2, 8, 13-14, and 16 were so rejected, *see* page 3 of that non-final Office Action. The Final Office Action appears to assert on pages 2-3 that these rejections are maintained. However, pages 4-5 of the Final Office Action appear to change the rejection to apply instead to only claims 8, 13-14, and 16. Because Appellant submits that the rejection is improper for all of the claims 1-2, 8, 13-14, and 16, Appellant addresses the rejection for all of these claims below even though it is unclear from the Final Office Action whether all of these claims actually stand rejected under 35 U.S.C. §102(e) as being anticipated by *Taylor*.

To anticipate a claim under 35 U.S.C. § 102, a single reference must teach every element of the claim, see M.P.E.P. § 2131. Appellant respectfully submits that claims 1-2, 8, 13-14, and 16 are not anticipated by *Taylor* because *Taylor* fails to teach each and every element of the claims, as discussed further below.

Independent Claim 1

Claim 1 recites in part "an operating system ... operable to execute an intrusion protection system management application, the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule" (emphasis added). *Taylor* fails to teach at least the above-emphasized element of claim 1, as discussed below.

Indeed, while the Final Office Action appears to allege on pages 2-3 thereof that *Taylor* teaches all elements of claim 1. The Final Office Action then, on page 7, appears to concede that *Taylor* fails to teach all elements of claim 1 in raising the rejection of claim 1 under 35 U.S.C. §103. As discussed below, *Taylor* does not teach all elements of claim 1.

Taylor does not teach a text-file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system (IPS) evaluates the network-exploit rule. Rather, *Taylor* appears to describe a configuration file that specifies to a firewall rules regarding whether a connection is permitted on particular ports, as well as rules regarding filtering packets for a permitted connection. *See* Col. 5, line 66 – Col. 6, line 60 of *Taylor*. While actions (e.g., filtering packets) for a given rule are only taken by the firewall if the corresponding rule is satisfied, the rules specified in the configuration file appear to all be evaluated by the firewall. *Taylor* does not teach that the configuration file comprises at least one field that includes information from which a determination is made as to whether an IPS evaluates the network-exploit rule. No determination of whether an intrusion protection system is to evaluate a rule is made in *Taylor*, but instead *Taylor* appears to teach that all rules defined in its configuration file are all evaluated irrespective of any information contained in the configuration file. Again, when evaluated, a determination may be made that a rule is not satisfied under certain circumstances, and thus the corresponding actions (e.g., filtering packets) may not be applied; but in all cases of *Taylor* all rules defined in the configuration file appear to be evaluated.

Thus, *Taylor* does not provide any teaching whatsoever of including at least one field in its configuration file from which a determination is made as to whether a network-exploit rule in the configuration file is to be evaluated by an IPS, which potentially leads to inefficient processing if rules are defined in the configuration file that are not desired to be evaluated, *see e.g.,* page 17, line 8 – page 21, line 2 of the specification of the present application.

In response to the above arguments, the Final Office Action asserts that *Taylor* discloses that the proxy determines which filter rule to apply, citing to col. 6, lines 30-50 and lines 58-60 of *Taylor*, *see* pages 2-3 of the Final Office Action. Appellant respectfully disagrees. First, it appears from the teaching of *Taylor* that the proxy may evaluate a rule to determine whether the rule is satisfied under certain circumstances (e.g., for a given connection), and if the rule is not satisfied, then the corresponding actions (e.g., filtering packets) of the rule are not applied (and thus the rule is not applied to the given connection); but in all cases of *Taylor* all rules defined in

the configuration file appear to be evaluated. In no case does *Taylor* provide any teaching whatsoever of its configuration file comprising "at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule", as recited by claim 1. And, the Examiner has failed to identify any teaching in *Taylor* of such a field in the configuration file. Thus, even if the proxy of *Taylor* does determine which rules to evaluate (which Appellant respectfully asserts above that the proxy does not), no disclosure has been identified in *Taylor* of a field in the configuration file from which such a determination is made.

In view of the above, *Taylor* fails to teach all elements of claim 1, and therefore claim 1 is not anticipated by *Taylor*. Therefore, Appellant respectfully requests that the rejection of claim 1 be overturned.

Dependent Claim 2

Dependent claim 2 depends from independent claim 1, and thus includes all of the limitations of claim 1 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 2 is allowable at least because of its dependence from claim 1 for the reasons discussed above.

Claim 2 further recites: "wherein the at least one field comprises a field selected from the group consisting of an ENABLED field and a SEVERITY field." *Taylor* further fails to teach that the field comprises such an ENABLED or SEVERITY field, as discussed further below with independent claim 8. Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 2 be overturned.

Independent Claim 8

Claim 8 recites in part "specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file." *Taylor* fails to teach at least this element of claim 8.

Taylor does not teach specifying an ENABLED field value or a SEVERITY level field value during generation of a text file. Rather, *Taylor* appears to describe a configuration file that specifies to a firewall rules regarding whether a connection is permitted on particular ports, as well as rules regarding filtering packets for a permitted connection. *See* Col. 5, line 66 – Col. 6, line 60 of *Taylor*. *Taylor* provides no teaching whatsoever of specifying an ENABLED field value or a SEVERITY level field value during generation of its configuration file. *Taylor* provides no teaching of such fields in its configuration file.

In rejecting claim 8, the non-final Office Action of April 7, 2006 relies upon its reasoning presented for claim 2, which cites to Col. 6, lines 31-57 and Col. 10, line 51 – Col. 11, line 32 of *Taylor* as teaching this element, *see* pages 3-4 of the non-final Office Action. The cited portions of *Taylor* are as follows:

> Another dynamic filter rule is a selective filtering rule. This rule requires proxy 211 to handle connection control packets and packet filters to handle the data packets. In other words, the packet filtering will be enabled only when proxy 211 has performed it's security checks for the connections, i.e., checking the relevant information on the SYN packet sent by DPF 207. For instance, this rule is useful for protocols such as File Transfer Protocol (FTP), which sends data packets on a different connection after establishing the connection. Other filtering rules are also possible such as not applying any filtering or applying a proxy filter at the application layer to all packets received on a specific connection.
>
> The configuration file discussed above, which stored the information on which ports are registered, further includes various filter rules to be applied for specific connections. For example, packets received from a particular port can be subjected to the filter all rule filter, while packets received from another port can be subjected to the selective filtering rule. The configuration file is preferably stored in the computer where firewall 201 is located. It should be noted, however, that the configuration file can be stored in any of internal hosts. It should also be noted that the system administrator creates the configuration information file discussed above and specifies the TPF rules by utilizing a graphical user interface configured receive appropriate information from the system administrator. (Col. 6, lines 31-57).

It should be noted that the above described program functions and associated data structure formats are implemented in computer programs such as C or C++. Alternatively, the computer programs can be written in other computer languages such as Pascal.

Referring back to FIG. 4, in order to continue on with the description of steps that take place during operation of firewall 201, in step 321, DPF 207 determines whether the packet matches with any of user specified rules. (This steps is performed when the port on which the communication establishing packet was received is not registered.) Whether the packet matches a user specified rule is determined by attribute information of the packet. The attribute information of the packet includes:

Source and destination computer addresses;

Source and destination transport layer protocol numbers;

Type of protocol (TCP, UDP etc.); and

Port numbers of NIC 203 on which the packet was received.

Anyone or a combination of the attributes can be utilized to determine if the packet matches with any user specified rules. Subsequently, if a user specified rule matches with the communication establishing packet, the matched rule is applied to the packet (step 323). If no user specified rule matches the packet, a transparency is applied (step 325).

The user specified rules 209 include user specified static filter rules and user specified dynamic filter rules.

Each entry in the user specified static filter rules includes the attributes discussed above and a value indicating the type of filter to apply to the packet. The types of filters include "permit" filter to forward the packet to its destination, "deny" to discard the packet, "absorb" to apply an application level filter and "a filter all rule" discussed above. In order to provide a finer granularity in the packet filtering, the packet filter of the present invention is extended to include additional fields such as:

(1) TCP flags (SYN, SYN-ACK, URG/PUSH) are provided to block new TCP connections from a certain host, but continue to allow packets of existing connections by adding a filter rule to deny SYN packets from the host; and

> (2) Unlike the conventional packet filter rules which only allow a single port to be specified in a rule, the present invention is also configured to allow/deny connections to a particular interface port range. For example, connections to X terminal ports can be denied by specifying a filter rule with the range of X terminal ports specified. (Col. 10, line 51 – Col. 11, line 32).

As can be seen, the relied-upon portions of *Taylor* make no mention whatsoever of specifying an ENABLED field value or a SEVERITY level field value during generation of its configuration file. No such field values are described as included in the configuration file. Further, no other portion of *Taylor* provides such teaching.

In response to the above arguments, the Final Office Action asserts that: "the 'allow/deny' field specifies the port to be filtered during generation of the text file that meets the recitation of the enabled field value." Page 3 of the Final Office Action. Appellant respectfully disagrees. As discussed above, *Taylor* discloses that "[e]ach entry in the user specified static filter rules includes the attributes discussed above and a value indicating the type of filter to apply to the packet." Col. 11, lines 11-13 of *Taylor*. "The types of filters include 'permit' filter to forward the packet to its destination, 'deny' to discard the packet, 'absorb' to apply an application level filter and 'a filter all rule' discussed above." Col. 11, lines 13-16 of *Taylor*. Thus, the allow/deny in *Taylor* refers to a part of the rule (or type of rule) indicating that the rule, when applied, discards or allows a packet. *Taylor* does not teach that this allow/deny type of rule constitutes an ENABLED field value or a SEVERITY level field value that is specified during generation of a text-file that defines a network-exploit rule. For instance, the allow/deny "type" of a rule in *Taylor* indicates whether the rule, when applied, filters/discards packets. Such allow/deny "type" of rule in *Taylor* does not constitute and ENABLED field that defines whether the rule is enabled. Instead, the allow/deny type of rule in *Taylor* in no way indicates whether the rule is enabled, but instead merely identifies whether the rule discards packets when the rule is satisfied/applied.

In view of the above, *Taylor* fails to teach all elements of claim 8, and therefore claim 8 is not anticipated by *Taylor*. Therefore, Appellant respectfully requests that the rejection of claim 8 be overturned.

Independent Claim 13 and Dependent Claims 14 and 16

Claim 13 recites in part "compiling the input into a machine-readable signature file comprising machine-readable logic representative of a network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field." *Taylor* fails to teach at least this element of claim 13.

Taylor does not teach compiling input into a machine-readable signature file that comprises a network-exploit rule and at least one of an ENABLED field and a SEVERITY field. Rather, *Taylor* appears to describe a configuration file that specifies to a firewall rules regarding whether a connection is permitted on particular ports, as well as rules regarding filtering packets for a permitted connection. *See* Col. 5, line 66 – Col. 6, line 60 of *Taylor*. *Taylor* provides no teaching whatsoever of such an ENABLED field or SEVERITY field in its configuration file, as discussed above with claim 8.

In view of the above, *Taylor* fails to teach all elements of claim 13, and therefore claim 13 is not anticipated by *Taylor*. Therefore, Appellant respectfully requests that the rejection of claim 13 be overturned.

Claims 14 and 16 each depend either directly or indirectly from independent claim 13, and thus inherit all limitations of independent claim 13. It is respectfully submitted that dependent claims 14 and 16 are allowable at least because of their dependency from independent claim 13 for the reasons discussed above.

C. Rejections under 35 USC §103 over *Taylor* in view of *Freund*

Additionally, claims 1-7, 9-12, 15, and 17-20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Taylor* in view of *Freund*. Appellant respectfully traverses these rejections for at least the reasons advanced below.

To establish a prima facie case of obviousness, three basic criteria must be met. *See* M.P.E.P. § 2143. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art references must teach or suggest all the claim limitations. Without conceding any other criteria, Appellant respectfully asserts that the applied combination of *Taylor* and *Freund* fails to teach or suggest all claim elements, as discussed below.

Independent Claim 1 and Dependent Claims 4-5 and 18

Claim 1 recites in part "an operating system ... operable to execute an intrusion protection system management application, the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule" (emphasis added). As discussed above, *Taylor* fails to teach at least the above-emphasized element of claim 1. Further, as discussed below, *Freund* also fails to teach or suggest at least this element, and thus the applied combination of *Taylor* and *Freund* fails to teach or suggest this element.

The Final Office Action relies upon *Freund* as disclosing the above element of claim 1, *see* pages 7-8 of the Final Office Action. The cited portions of *Freund* appear to disclose that access rules can be defined for restricting the access of individual users, workgroups, or an entire organization of certain sites, *see e.g.,* Col. 5, line 30 – col. 6, line 28, and col. 8, line 40 – col. 9, line 36 of *Freund*. *Freund* discloses that the rules are stored to a rules database (*see* col. 20, line 50 – col. 21, line 40, and Figure 5 of *Freund*). *Freund* appears to disclose that a special user interface, such as that shown in Figures 7A-7K, is used to present and receive information to/from a user regarding the rules. As discussed below, *Freund* fails to teach or suggest at least the above-identified element of claim 1.

First, *Freund* fails to teach or suggest a "text-file defining a network-exploit rule" (emphasis added), as recited by claim 1. Nothing in *Freund* suggests that the access rules are defined in a text-file. Rather, a special user interface (as shown in Figures 7A-7K of *Freund*) appears to be required to enable a user to input information for defining a rule, which is then stored to the rules database (presumably in a format other than as a text-file, but instead in some format that can be read and output by the special user interface). Again, *Freund* simply appears to provide no teaching or suggestion of a text-file defining a network-exploit rule, but instead appears to propose a system that requires a special user interface for reading from and writing to the access rules.

Because a text-file is not taught or suggested by *Freund*, *Freund* fails to teach or suggest that the text-file comprises at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule. At col. 5, lines 42-43, *Freund* mentions that its proposed methodology includes "[t]ransmitting a filtered subset of the rules to the particular client computer". However, *Freund* provides no teaching or suggestion that such filtering of a subset of the rules that are to be sent to a particular client computer is performed based on at least one field included in a text-file that defines the rules. Further, the Final Office Action notes that col. 24, lines 42-44 of *Freund* states that: "Enforcement of any given rule can be suspended by "disabling" the rule, such as shown at 724." However, this is not referring to any field of a text-file, but instead appears to suggest that a special user interface, such as that shown with Figures 7A-7K of *Freund*, can be used for disabling a rule. In any case, *Freund* simply provides no mention of a text-file defining rules, and *Freund* certainly fails to provide any teaching or suggestion that a text-file defining rules comprises a field that includes information from which a determination is made as to whether an intrusion protection system evaluates the rule. Any disabling of a rule suggested by *Freund* is not made in a field of a text-file, but instead appears to be made through interaction with a special user interface.

In view of the above, the combination of *Taylor* and *Freund* fails to teach or suggest all elements of claim 1, and therefore claim 1 is not obvious over this combination of references. Therefore, Appellant respectfully requests that the rejection of claim 1 be overturned.

Claims 4-5 and 18 each depend either directly or indirectly from independent claim 1, and thus inherit all limitations of independent claim 1. It is respectfully submitted that dependent claims 4-5 and 18 are allowable at least because of their dependency from independent claim 1 for the reasons discussed above.

Dependent Claim 2

Dependent claim 2 depends from independent claim 1, and thus includes all of the limitations of claim 1 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 2 is allowable at least because of its dependence from claim 1 for the reasons discussed above.

Claim 2 further recites: "wherein the at least one field comprises a field selected from the group consisting of an ENABLED field and a SEVERITY field." The combination of *Taylor* and *Freund* further fails to teach or suggest that the field of the text-file comprises such an ENABLED or SEVERITY field. The Office Action appears to rely on *Taylor* as disclosing this further element of claim 2. However, as discussed above (e.g., with claim 8), *Taylor* fails to teach or suggest this further element of claim 2. Additionally, as discussed above, *Freund* fails to teach or suggest any text-file that defines network-exploit rules, and certainly fails to teach or suggest a text-file that comprises an ENABLED or SEVERITY field.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 2 be overturned.

Dependent Claim 3

Dependent claim 3 depends from independent claim 1, and thus includes all of the limitations of claim 1 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 3 is allowable at least because of its dependence from claim 1 for the reasons discussed above.

Claim 3 further recites: "wherein the node is operable to compile the text-file into a machine-readable signature-file and transmit the machine-readable signature-file to at least one other node of the network." The applied combination of *Taylor* and *Freund* fails to teach or suggest this further element of claim 3. Neither *Taylor* nor *Freund* teaches or suggests compiling a text-file into a machine-readable signature-file. For instance, as discussed above, *Freund* fails to teach or suggest any text-file, but instead appears to disclose that rules are stored to a machine-readable file that can be read by a special user interface, such as that of Figures 7A-7k of *Freund*. *Freund* certainly fails to teach or suggest compiling a text-file that defines network-exploit rules into a machine-readable signature-file. *Taylor* likewise fails to teach or suggest this element.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 3 be overturned.

Dependent Claim 6

Dependent claim 6 depends from claim 5, which depends from claim 2, which depends from independent claim 1. Thus, claim 6 includes all of the limitations of claims 1, 2, and 5 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 6 is allowable at least because of its dependence from claims 1 and 2 for the reasons discussed above.

Claim 5 recites "the management application operable to transmit a subset of the plurality of machine-readable signature-files to another node connected to the network." Claim 6 further recites: "wherein the subset comprises all machine-readable signature-files of the plurality of

machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value." The combination of *Taylor* and *Freund* fails to teach or suggest this further element of claim 6.

The Final Office Action appears to contend that *Freund* discloses this element of claim 6, *see* pages 9-10 of the Final Office Action. However, as discussed above, *Freund* does not disclose a text-file that defines network-exploit rules, and thus *Freund* does not disclose machine-readable signature-files that are generated from respective text-files. Further, *Freund* provides no teaching or suggestion of a text-file that has an asserted ENABLED field value, and *Freund* provides no teaching or suggestion of transmitting a subset of machine-readable signature-files that are generated from text-files having such an asserted ENABLED field value. While, at col. 5, lines 42-43, *Freund* mentions that its proposed methodology includes "[t]ransmitting a filtered subset of the rules to the particular client computer", *Freund* provides no teaching or suggestion that such filtering of a subset of the rules that are to be sent to a particular client computer is performed based on an asserted ENABLED field in a text-file from which the machine-readable signature-files are generated.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 6 be overturned.

Dependent Claim 7

Dependent claim 7 depends from claim 5, which depends from claim 2, which depends from independent claim 1. Thus, claim 7 includes all of the limitations of claims 1, 2, and 5 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 7 is allowable at least because of its dependence from claims 1 and 2 for the reasons discussed above.

Claim 5 recites "the management application operable to transmit a subset of the plurality of machine-readable signature-files to another node connected to the network." Claim 7 further recites: "wherein the management application is operable to accept a SEVERITY threshold from the input device and the subset comprises all machine-readable signature-files respectively

generated from a text-file having a SEVERITY field value equal to or greater than the threshold." The combination of *Taylor* and *Freund* fails to teach or suggest this further element of claim 7.

The Final Office Action appears to contend that *Freund* discloses this element of claim 7, *see* page 10 of the Final Office Action. However, as discussed above, *Freund* does not disclose a text-file that defines network-exploit rules, and thus *Freund* does not disclose machine-readable signature-files that are generated from respective text-files. Further, *Freund* provides no teaching or suggestion of a text-file that has a SEVERITY field value, and *Freund* provides no teaching or suggestion of transmitting a subset of machine-readable signature-files that are generated from text-files having such a SEVERITY field value equal to or greater than a threshold. While, at col. 5, lines 42-43, *Freund* mentions that its proposed methodology includes "[t]ransmitting a filtered subset of the rules to the particular client computer", *Freund* provides no teaching or suggestion that such filtering of a subset of the rules that are to be sent to a particular client computer is performed based on a SEVERITY field value in a text-file from which the machine-readable signature-files are generated.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 7 be overturned.

Dependent Claims 9-10 and 19-20

Dependent claims 9-10 and 19-20 depend either directly or indirectly from independent claim 8, and thus inherit all limitations of claim 8. As discussed above, *Taylor* fails to teach all elements of independent claim 8. Further, *Freund* is not relied upon as teaching or suggesting the above-identified elements of claim 8 lacking from *Taylor*, nor does it do so. Thus, it is respectfully submitted that dependent claims 9-10 and 19-20 are allowable at least because of their dependency from independent claim 8 for the reasons discussed above.

Dependent Claim 11

Dependent claim 11 depends indirectly from independent claim 8, and thus includes all of the limitations of claim 8 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 11 is allowable at least because of its dependence from claim 8 for the reasons discussed above.

Claim 10 recites "transmitting, by a management node of the network, a subset of the plurality of machine-readable signature-files to a node in the network." Claim 11 depends from claim 10 and further recites: "wherein the subset of machine-readable signature-files comprises all of the plurality of machine-readable signature-files each generated from a respective one of the plurality of text-files that has the respective ENABLED field asserted." The combination of *Taylor* and *Freund* fails to teach or suggest this further element of claim 11.

The Final Office Action appears to contend that *Freund* discloses this element of claim 11, *see* pages 9-10 of the Final Office Action. However, as discussed above, *Freund* does not disclose a text-file that defines network-exploit rules, and thus *Freund* does not disclose machine-readable signature-files that are generated from respective text-files. Further, *Freund* provides no teaching or suggestion of a text-file that has an asserted ENABLED field value, and *Freund* provides no teaching or suggestion of transmitting a subset of machine-readable signature-files that are generated from text-files having such an asserted ENABLED field value. While, at col. 5, lines 42-43, *Freund* mentions that its proposed methodology includes "[t]ransmitting a filtered subset of the rules to the particular client computer", *Freund* provides no teaching or suggestion that such filtering of a subset of the rules that are to be sent to a particular client computer is performed based on an asserted ENABLED field in a text-file from which the machine-readable signature-files are generated.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 11 be overturned.

Dependent Claim 12

Dependent claim 12 depends indirectly from independent claim 8, and thus includes all of the limitations of claim 8 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 12 is allowable at least because of its dependence from claim 8 for the reasons discussed above.

Claim 10 recites "transmitting, by a management node of the network, a subset of the plurality of machine-readable signature-files to a node in the network." Claim 12 depends from claim 10 and further recites: "specifying a priority level threshold, the subset of the plurality of machine-readable signature-files comprised of all machine-readable signature-files generated from a respective one of the plurality of text-files having a SEVERITY level field value equal to or greater than the threshold." The combination of *Taylor* and *Freund* fails to teach or suggest this further element of claim 12.

The Final Office Action appears to contend that *Freund* discloses this element of claim 12, *see* page 10 of the Final Office Action. However, as discussed above, *Freund* does not disclose a text-file that defines network-exploit rules, and thus *Freund* does not disclose machine-readable signature-files that are generated from respective text-files. Further, *Freund* provides no teaching or suggestion of a text-file that has a SEVERITY level field value, and *Freund* provides no teaching or suggestion of transmitting a subset of machine-readable signature-files that are generated from text-files having such a SEVERITY level field value equal to or greater than a threshold. While, at col. 5, lines 42-43, *Freund* mentions that its proposed methodology includes "[t]ransmitting a filtered subset of the rules to the particular client computer", *Freund* provides no teaching or suggestion that such filtering of a subset of the rules that are to be sent to a particular client computer is performed based on a SEVERITY level field value in a text-file from which the machine-readable signature-files are generated.

Therefore, for this further reason, Appellant respectfully requests that the rejection of claim 12 be overturned.

Dependent Claims 15 and 17

Dependent claims 15 and 17 depend either directly or indirectly from independent claim 13, and thus inherit all limitations of claim 13. As discussed above, *Taylor* fails to teach all elements of independent claim 13. Further, *Freund* is not relied upon as teaching or suggesting the above-identified elements of claim 13 lacking from *Taylor*, nor does it do so. Thus, it is respectfully submitted that dependent claims 15 and 17 are allowable at least because of their dependency from independent claim 13 for the reasons discussed above.

D. Conclusion

In view of the above, Appellant requests that the board overturn the outstanding rejections of claims 1-20. Attached hereto are a Claims Appendix, Evidence Appendix, and Related Proceedings Appendix. As noted in the attached Evidence Appendix, no evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted. Also, as noted by the Related Proceedings Appendix, no related proceedings are referenced in II above, and thus no copies of decisions in related proceedings are provided.

No fee is believed to be due with this Appeal Brief. If any additional fee is due, please charge Deposit Account No. 08-2025, under order No. 10017334-1 from which the undersigned is authorized to draw.

Dated: January 8, 2007

Respectfully submitted,

By _____
Jody C. Bishop
Registration No.: 44,034
(214) 855-8007
(214) 855-8200 (Fax)

VIII – CLAIMS APPENDIX

Claims Involved in the Appeal of Application Serial No. 10/003,820:

1. A node of a network for managing an intrusion protection system, the node comprising:

a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit; and

an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application, the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule.

2. The node according to claim 1, wherein the at least one field comprises a field selected from the group consisting of an ENABLED field and a SEVERITY field.

3. The node according to claim 1, wherein the node is operable to compile the text-file into a machine-readable signature-file and transmit the machine-readable signature-file to at least one other node of the network.

4. The node according to claim 1, further comprising a database, the node operable to store a plurality of text-files, each respectively defining a network-exploit rule, in the database.

5. The node according to claim 2, further comprising a machine-readable signature-file database operable to store a plurality of machine-readable signature-files each generated from one of a respective plurality of text-files, the management application operable to transmit a subset of the plurality of machine-readable signature-files to another node connected to the network.

6. The node according to claim 5, wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value.

7. The node according to claim 5, wherein the management application is operable to accept a SEVERITY threshold from the input device and the subset comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than the threshold.

8. A method of distributing command and security updates in a network having an intrusion protection system, comprising:

generating a text-file defining a network-exploit rule; and

specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file.

9. The method according to claim 8, further comprising storing a plurality of text-files in a database, each text-file defining a network-exploit rule.

10. The method according to claim 9, further comprising transmitting, by a management node of the network, a subset of the plurality of machine-readable signature-files to a node in the network.

11. The method according to claim 10, wherein the subset of machine-readable signature-files comprises all of the plurality of machine-readable signature-files each generated from a respective one of the plurality of text-files that has the respective ENABLED field asserted.

12. The method according to claim 10, further comprising specifying a priority level threshold, the subset of the plurality of machine-readable signature-files comprised of all machine-readable signature-files generated from a respective one of the plurality of text-files having a SEVERITY level field value equal to or greater than the threshold.

13. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

reading input from an input device of the computer;

compiling the input into a machine-readable signature file comprising machine-readable logic representative of a network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field;

evaluating the machine-readable signature file; and

determining the value of the at least one field of the machine-readable signature file.

14. The computer readable medium according to claim 13, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of specifying a SEVERITY threshold value.

15. The computer readable medium according to claim 14, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of transmitting the machine-readable signature file to another node of the network upon determining the value of the SEVERITY field is greater than the threshold.

16. The computer readable medium according to claim 13, further comprising a set of instruction that, when executed by the processor, cause the processor to perform the computer method of generating a text-file from the input, the text-file specifying the network-exploit rule and the at least one field, the machine-readable signature file compiled from the text file.

17. The computer readable medium according to claim 13, further comprising a set of instruction that, when executed by the processor, cause the processor to perform the computer method of transmitting the machine-readable signature file to another node of the network upon determining the ENABLED field value is logically asserted.

18. The node according to claim 1 wherein the intrusion protection system management application is further operable to determine, based at least in part on the at least one field, ones of a plurality of other nodes to which the network-exploit rule is to be distributed.

19. The method according to claim 8 wherein the ENABLED field value specifies whether the network-exploit rule is enabled for evaluation by an intrusion protection system, and wherein the SEVERITY level field value specifies a severity level of the network-exploit rule.

20. The method according to claim 8 further comprising:

distributing the network-exploit rule and the at least one field to a plurality of nodes; and

determining by an intrusion protection system of each of the plurality of nodes, based at least in part on the at least one field, whether to evaluate the network-exploit rule in protecting the intrusion protection system's respective node.

IX. EVIDENCE APPENDIX

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

X. RELATED PROCEEDINGS APPENDIX

No related proceedings are referenced in II above, and thus no copies of decisions in related proceedings are provided.